

### **REMARKS**

Reconsideration and allowance of the subject patent application are respectfully requested.

Amendments of a formal nature have been made to claims 5, 13 and 16. These amendments are not made for reasons relating to patentability.

Claims 1, 2, 4-6, 8 and 13-17 were rejected under 35 U.S.C. Section 102(b) as allegedly being "anticipated" by Roberts et al. (U.S. Patent Publication No. 2004/0088570). This rejection is respectfully traversed at least for the following two independent reasons.

First, Applicant denies that Roberts et al. discloses feature (c) of claims 1 and 5 of using a content scanner to scan an external object and to determine the acceptability of the object according to predefined rules, responsive to a request to retrieve the external object from the targets.

Second, the two parts of the disclosure of Roberts et al. relied on in the office action as meeting the requirements of features (b) and (c) of claims 1 and 5 are not disclosed in combination, such that there is in fact no lack of novelty.

These two reasons are discussed in greater detail below.

With regard to the first reason for the deficiencies of Roberts et al., feature (c) of claim 5 recites:

responsive to a request to retrieve an external object from one of said targets on the trusted server, using a content scanner to scan the external object ... and to determine the acceptability of the object according to predefined rules.

Claim 1 includes a similar recitation.

The office action references the disclosure of step 42 at paragraph [0037], lines 1-6 of Roberts et al. as allegedly disclosing this feature. This is also discussed in paragraph 5 of the office action. The referenced disclosure relates to an operation performed in response to a request to access an URL, which can be viewed as "a request to retrieve an external object" in the claims. However, Applicant strongly contests that this operation meets the requirements of the claims.

The operation described at paragraph [0037], lines 1-6 of Roberts et al. is to make "a check as to whether the content associated with that address has changed since it was scanned."

Roberts et al. subsequently discloses that “[o]ne way of achieving this is to checksum the webpage when it was pre-emptively scanned, store that checksum and then compare that checksum against a new checksum derived from the retrieved webpage when the user requests access.” However, Applicant respectfully submits that such a check of whether a webpage has changed does not constitute the feature of claims 1 and 5 of using “a content scanner to scan the external object ... and to determine the acceptability of the object according to predefined rules.”

First, a “scan” of an object requires some actual examination of the object itself, which is not met by simply deriving a checksum for the external object.

Second, this distinction is evident from the context of the disclosure in Roberts et al. Roberts et al. itself relates to a content scanning. This is the process performed in step 28 of Figure 3, example (see paragraph [0032]). However, Roberts et al. does not use the term “scan” when describing step 42 of making a check as to whether the content has changed since it was scanned. This is because there is a clear technical distinction between (1) content scanning as this term is used in the subject patent application and in Roberts et al. and (2) merely checking to see whether a webpage has changed. This distinction is clear in the context of Roberts et al. because the whole aim of the teaching of Roberts et al. is to speed up the retrieval of the object by avoiding the need to perform such a scan when the webpage is retrieved. It is therefore clear that the check as to whether the webpage has changed disclosed in paragraph [0037], lines 1-6 is of an entirely different technical nature in that it does not take as long as the previously performed scan. Otherwise the entire benefit of the pre-emptive scan would be lost.

The second reason for the deficiency of Roberts et al. is independent of the above-discussed first reason. That is, the second reason constitutes an additional basis for the failure of Roberts et al. to anticipate the pending claims.

Specifically, the two portions of Roberts et al. relied on in the office action as disclosing features (b) and (c) of claims 1 and 5 are not disclosed in Roberts et al. as being applied in combination. This point is explained further below.

Regarding feature (b), the office action relies on the disclosure at paragraph [0034], lines 10-18. Paragraph [0034] as a whole describes step 38 which is the action taken after performance of the pre-emptive scan of a webpage (i.e., an external object) which is the target of a hyperlink. Paragraph [0034] describes several alternative actions. Paragraph [0034], lines 1-7

describes a first action taken when the webpage (i.e., external object) has been found not to contain malware. In this case, the internet address of the external object is stored in a database. Paragraph [0034], lines 10-18 (on which the office action relies) describes a second, alternative action which occurs when the webpage (i.e., external object) is found to contain malware. In this case, the action is to prepare a cleaned version of the data and to store that cleaned version locally. Clearly the first action described in paragraph [0034], lines 1-7 does not meet the requirement of feature (b). For the sake of the discussion in this response, it is assumed that the second action described at paragraph [0034], lines 10-18 meets the requirement of feature (b).

Regarding feature (c), the office action relies on the disclosure at paragraph [0037], lines 1-6. Paragraph [0037] as a whole describes step 42 which is the action taken when the hyperlink is followed (i.e., on receipt of a request to retrieve an external object). Paragraph [0037] describes several alternative actions.

Paragraph [0037], lines 1-6 describe a first action taken when a webpage (i.e., external object) has been found not to contain malware. This action is to check whether the webpage has changed since it was pre-emptively scanned. It is clear in the overall context of the disclosure of Roberts et al. that this first action described at paragraph [0037], lines 1-6 is performed only in the case that step 38 comprises the first action of storing the internet address of a webpage (i.e., external object) which was found not to contain malware as described at paragraph [0034], lines 1-7. This first action in step 42 is not necessary in combination with the second action of step 38 described at paragraph [0034], lines 10-18. Clearly, it is not necessary to perform the first action in step 42 of checking whether the content associated with an address has changed in the case that a clean version of the data has been prepared and stored locally in accordance with the second action of step 38 described at paragraph 34, lines 10-18.

This point is made clearer to the skilled reader by the subsequent disclosure in paragraph [0037] of a second, alternative action to be performed in step 42 in combination with the performance of the second action in step 38 of storing a cleaned version of a webpage which is found to contain malware. The relevant disclosure of paragraph [0037] is as follows. After describing making a check as to whether the content has changed in the case that the webpage was one that had been pre-scanned and found not to contain malware (see paragraph [0037],

lines 1-6), paragraph [0037] goes on to describe how the checking may be performed. In paragraph [0037], lines 18-23, the statement is made:

Other possibilities would be that a cleaned version of the webpage that had previously been found to contain malware could have been prepared and stored locally to be supplied in place of the infected webpage when a request to access that infected webpage was made.

This is an express disclosure of the action taken when step 38 consists of the second action. It is clear from the context and the words “other possibilities” that this second action described in paragraph [0037], lines 18-23 is performed as an alternative to the first action described at paragraph [0037], lines 1-6.

In overview, Roberts et al. discloses two alternatives.

The first alternative performed in the case that the webpage is found not to contain malware in the pre-emptive scan is that (1) step 38 comprises the first action described at paragraph [0034], lines 1-7 and (2) step 42 comprises the first action described at paragraph [0037], lines 1-6. In this first alternative, there is no action corresponding to feature (b).

The second alternative performed in the case that the webpage is found to contain malware content in the pre-emptive scan is that (1) step 38 comprises the second action described in paragraph [0034], lines 10-18 and (2) step 48 comprises the second action described at paragraph [0037], lines 18-23. This second alternative comprises action in step 38 that might be viewed as corresponding to feature (b). However, given that feature (c) recites scanning responsive to “receipt of a request to retrieve an external object from one of said targets on the trusted server,” the second alternative does not involve any action corresponding to feature (c), because in the second alternative the cleaned webpage is simply supplied without any further scan.

For at least these reasons, Applicant respectfully submits that Roberts et al. cannot anticipate claims 1 and 5 or the claims that depend therefrom.

Claims 15 and 17 distinguish from Roberts et al. for similar reasons. Moreover, claims 15 and 17 recite, inter alia, identifying first hyperlinks in contents of electronic documents; modifying the electronic documents by replacing the identified first hyperlinks with different second hyperlinks which point to a trusted server; storing data to relate the second hyperlinks to the first hyperlinks; and in response to a request received by the trusted server when one of the

second hyperlinks is selected, using the stored data to determine the first hyperlink corresponding to the selected second hyperlink and retrieving an object using the determined first hyperlink. The collective discussion of claims 1, 5, 15 and 17 in the office action does not address, for example, the claims 15 and 17 features of storing data to relate the second hyperlinks to the first hyperlinks or of using the stored data when a second hyperlink is selected to determine the corresponding first hyperlink and then retrieving an object using the determined first hyperlink. Paragraph [0034] of Roberts et al. mentions replacing an original internet address with an address pointing to clean data at a new location. However, there is no disclosure in Roberts of storing data relating the original and new addresses, much less of responding to a request for the new location by determining the original location and then retrieving an object from the first location. Indeed, in Roberts et al. the new location is provided when the object at the original location is determined to contain malware. It does not make sense that Roberts et al. would receive a request for the “clean” object at the new location and, instead of providing the clean version, retrieve the malware-containing version at the original address. For the additional and independent reasons that Roberts et al. does not disclose storing data to relate the second hyperlinks to the first hyperlinks or using the stored data as set forth in claims 15 and 17, Roberts et al. cannot anticipate these claims or any claims that depend therefrom.

Claims 3 and 7 were rejected under 35 U.S.C. Section 103(a) as allegedly being made “obvious” by Roberts et al. in view of Lambert et al. (U.S. Patent No. 6,629,138). Lambert et al. is applied for its alleged disclosure relating to recursion. Among other things, Lambert et al. does not remedy the deficiencies of Roberts et al. with respect to claims 1 and 5, from which claims 3 and 7 respectively depend. Moreover, Applicant submits that the office action overstates the teaching of Lambert et al. The referenced portion of Lambert et al. relates to creating a table of contents (TOC) and Applicant does not find any reference to flagging a document as unacceptable as suggested in the office action.


New claims 18 and 19 have been added. These new claims find support in the original disclosure (see, e.g., page 2, lines 13-17) and the Examiner is invited to independently confirm that this is the case. These claims depend from claim 15 and patentably distinguish from the applied references because of these dependencies and because of the additional patentable features recited therein.

SHIPP, A.  
Appl. No. 10/500,958  
Response to Office Action dated October 4, 2007

The pending claims are believed to be allowable and favorable office action is respectfully requested.

Respectfully submitted,

**NIXON & VANDERHYE P.C.**

By:   
Michael J. Shea  
Reg. No. 34,725

MJS:mjs  
901 North Glebe Road, 11th Floor  
Arlington, VA 22203-1808  
Telephone: (703) 816-4000  
Facsimile: (703) 816-4100